Een eerste verkenning van het voorstel verordening bescherming persoonsgegevens

Cuijpers, C.M.K.C.; van Eecke, P.; Kindt, E.; de Vries, H.

Published in:
Computerrecht

Publication date:
2012

Document Version
Peer reviewed version

Artikelen

<Computerrecht 2012/78>

Een eerste verkenning van het Voorstel Verordening bescherming persoonsgegevens

Colette Cuijpers[1], Patrick van Eecke[2], Els Kindt[3] en Hester de Vries[4]

De lidstaten van de Europese Unie staan aan de vooravond van een grondige wijziging van de regelgeving op het gebied van bescherming van persoonsgegevens. De Europese Commissie maakte daaromtrent op 25 januari 2012 haar voorstellen bekend, waaronder het voorstel van een Verordening inzake de bescherming van personen bij de verwerking van persoonsgegevens. Dit Voorstel beoogt een einde te maken aan de soms aanzienlijke verschillen tussen de wetgeving in de lidstaten van de EU en de verschillen in interpretatie en handhaving door toezichthouders. Het internationale bedrijfsleven stuurde hierop sedert enige tijd aan. Maar er worden ook diverse nieuwe verplichtingen geïntroduceerd en op diverse punten worden de regels aangescherpt, niet alleen voor verantwoordelijken, maar ook voor verwerkers.[5] Tegelijkertijd worden de rechten van de betrokkenen geactualiseerd en versterkt. De strekking van diverse bepalingen is evenwel nog onzeker. Duidelijk is wel dat de toezichthouders meer 'tanden' krijgen. Alle reden om de ontwikkelingen kritisch te volgen. Dit artikel biedt een eerste verkenning van het Voorstel.

Inleiding

Op 25 januari 2012 publiceerde de Europese Commissie het Voorstel van een Verordening betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrij verkeer van die gegevens[6] (hierna 'het Voorstel').[7] Het Voorstel is onderdeel van een pakket aan maatregelen, waarmee de Europese Commissie harmonisatie van de privacyregelgeving beoogt. Het nieuwe juridisch raamwerk voor de bescherming van persoonsgegevens in de Unie omvat ook een ontwerprichtlijn voor gegevensbescherming in de rechtshandhavingssector.[8] Bij de nieuwe voorstellen heeft de Commissie eveneens een werkdocument uitgegeven waarin zij de verschillende

[1] Dr. Colette Cuijpers is als senior onderzoeker verbonden aan TILT – Tilburg Institute for Law, Technology, and Society, Tilburg University.
[2] Prof. dr. Patrick Van Eecke doceert ICT-recht aan de Universiteit Antwerpen en is tevens visiting professor aan Queen Mary University, London.
[3] Dr. Els Kindt is als postdoctoraal onderzoeker verbonden aan ICRI – KU Leuven – IBBT.
[4] Dr. Hester de Vries is advocaat bij Kennedy Van der Laan en tevens als docent verbonden aan de afdeling Transnational Legal Studies van de Vrije Universiteit.
[5] In plaats van verwerker wordt in Nederland veelal gesproken van ´bewerker´.
[6] European Commission, 'Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)', COM(2012) 11 final, 25.01.2012, 118 p.
[7] Het voorstel is inmiddels ook in het Nederlands beschikbaar via: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_nl.pdf.
[8] European Commission, 'Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data', COM(2012) 10 final, 25.01.2012, 54 p.

beleidsobjectieven en de mogelijkheden om deze uit te voeren omstandig heeft beschreven en vergeleken.[9] Interessant is ook om te weten dat ondertussen een groep van experts is aangevangen met de herziening van Conventie nr. 108 van de Raad van Europa. Deze Conventie tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens van 1981 bevatte als eerste bindend document in het domein van gegevensbescherming de principes die later als basis zouden dienen voor de Richtlijn 95/46/EC. In dit artikel beperken wij ons tot het eerdergenoemde Voorstel Verordening bescherming persoonsgegevens.

De Verordening zal in de plaats treden van de Richtlijn bescherming persoonsgegevens (95/46/EC), die dateert uit 1995. Het behoeft geen betoog dat de wereld waarin wij nu leven aanzienlijk verschilt van die in 1995. De Commissie wijst erop dat de technologische ontwikkelingen, waaronder bijvoorbeeld het internet, nieuwe uitdagingen hebben gecreëerd voor de bescherming van persoonsgegevens. De schaal waarop persoonsgegevens worden gedeeld en verzameld is spectaculair toegenomen, zowel in de private als in de publieke sector. Individuen maken hun persoonsgegevens in toenemende mate publiek en wereldwijd toegankelijk. De technologie heeft zowel de economie als het sociale leven veranderd.

In de preambule bij het Voorstel worden de redenen voor de introductie van het nieuwe juridische raamwerk uiteengezet. De Europese Commissie stelt dat het vergroten van het vertrouwen in de online-omgeving van doorslaggevende betekenis is voor de economische ontwikkelingen. Gebrek aan vertrouwen heeft tot gevolg dat consumenten terughoudend zullen zijn om online te kopen en nieuwe diensten te aanvaarden. Dit brengt het gevaar mee dat de ontwikkeling van innovatief gebruik van nieuwe technologieën wordt vertraagd. Om al deze redenen speelt bescherming van persoonsgegevens een centrale rol in de Digitale Agenda voor Europa en de Europa 2020 Strategie.[10]

Doeleinden van de in 1995 aangenomen Richtlijn waren enerzijds de bescherming van het fundamentele recht op bescherming van persoonsgegevens en anderzijds het garanderen van het vrije verkeer van persoonsgegevens tussen de lidstaten. De Richtlijn diende door middel van wetgeving te worden geïmplementeerd in het nationale recht van de lidstaten. In de praktijk bleken aanzienlijke verschillen te bestaan tussen de wijze waarop de Richtlijn in het nationale recht werd geïmplementeerd. De bepaling inzake toepasselijk recht leidde er in de praktijk toe dat een multinational met vestigingen in 27 EU-lidstaten in ieder van de lidstaten aan het nationaal toepasselijke recht diende te voldoen. Dit leidde bijvoorbeeld tot de noodzaak om documenten zoals een privacystatement te laten aanpassen aan de wetgeving van 27 lidstaten vanwege (kleine, maar soms ook grote) verschillen tussen het nationaal toepasselijke recht. Daarnaast leidde dit onder andere tot 27 (verschillende) meldingen en contacten met toezichthouders, met ieder eigen interpretaties en een eigen handhavingsbeleid.

Er bestond verder geen eenduidige interpretatie van de definities in de Richtlijn en evenmin duidelijkheid omtrent de kernbepaling inzake het toepasselijk recht, hetgeen in de praktijk leidde tot rechtsonzekerheid.

"The rules in Article 4(1)a are quite simply utterly confused and impossible to apply in the new global-technical environment. Not surprisingly, the rules are applied differently in the Member States, leading to conflicts of law (which are only not too serious in practice because the competing and conflicting laws on paper are often not enforced in practice)"

[9] Zie Europese Commissie, 'Commission Staff Working Paper. Impact Assessment', SEC(12) 72 final, 25.1.2012, 153 p., beschikbaar via: http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=SEC:2011:0580:FIN:EN:PDF.

[10] Beide genoemde beleidsdocumenten van de Europese Commissie zijn beschikbaar via: http://ec.europa.eu/information_society/digital-agenda/publications/index_en.htm.

aldus een van de conclusies van een in opdracht van de Europese Commissie uitgevoerd rechtsvergelijkend onderzoek.[11] Sinds 2007, dat wil zeggen vele jaren na de totstandkoming van de Richtlijn, heeft de Artikel 29 Werkgroep nog een reeks van opinies en adviezen gepubliceerd, waarin onder meer de kernbegrippen 'persoonsgegevens', 'verantwoordelijke en verwerker' en 'toestemming' nader worden toegelicht. Daarmee beoogde de Artikel 29 Werkgroep bij te dragen aan een uniforme uitleg van deze begrippen.[12] Deze inspanningen ten spijt, bleven de verschillen in de wetgeving van 27 lidstaten echter bestaan.

In 2009 lanceerde de Europese Commissie bijgevolg een Consultatie om de doeltreffendheid van de Richtlijn in kaart te brengen en daarna in 2010 een Consultatie betreffende een alomvattende benadering van bescherming van persoonsgegevens in de Unie en tal van gerichte consultaties met key-stakeholders.[13] In 2011 werden diverse workshops georganiseerd, waaronder een bijeenkomst met de toezichthouders op het gebied van bescherming persoonsgegevens. Het resultaat is de keuze voor een alomvattend raamwerk voor de bescherming van persoonsgegevens en de keuze voor de algemene Verordening als regelgevend instrument. Naar het oordeel van de Commissie is een Verordening noodzakelijk om rechtszekerheid en transparantie te bieden voor ondernemers, inclusief micro-ondernemers en het midden- en kleinbedrijf; om betrokkenen hetzelfde niveau van juridisch afdwingbare rechten te bieden en verantwoordelijken en verwerkers hetzelfde niveau van verplichtingen en verantwoordelijkheden te geven; om consistent toezicht en handhaving te garanderen en om effectieve samenwerking van de toezichthouders in de verschillende lidstaten te realiseren.[14] Gegeven de ervaringen met de (omzetting van de) Richtlijn is de keuze voor een Verordening als regelgevend instrument logisch. Nu een Verordening directe werking heeft, wordt voorkomen dat uiteenlopende wetgeving in de lidstaten ontstaat. Anderzijds bevat het huidige Voorstel zo veel uitzonderingen die de lidstaten toelaten om toch nationale wetgeving uit te vaardigen dat men zich kan afvragen in welke mate het harmoniserend karakter van de ontwerpverordening behouden kan blijven.[15]

De juridische basis voor de Verordening vormt art. 16 VWEU,[16] zoals geïntroduceerd door het Verdrag van Lissabon.[17] Het Voorstel doorloopt de gewone wetgevingsprocedure (art. 294

[11] European Commission, 'Final Report, Comparative Study on different approaches to new privacy challenges, in particular in the light of technological developments, submitted by LRDP Kantor Ltd in association with Centre for Public Reform', 20.01.2010, beschikbaar via: http://ec.europa.eu/justice/policies/privacy/studies/index_en.htm. Zie tevens European Commission, 'Legal analysis of a single market for the information society, The future of on-line privacy and data protection', DLA Piper, 30 May 2011, beschikbaar via http://ec.europa.eu/information_society/newsroom/cf/itemdetail.cfm?item_id=7022.

[12] Opinies en adviezen beschikbaar via: http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm.

[13] Zie bijv. de input geleverd door de Artikel 29 Werkgroep 'The Future of Privacy. Joint Contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data', 1.12.2009, WP 168 en beschikbaar via: http://ec.europa.eu/justice/news/consulting_public/news_consulting_0006_en.htm.

[14] Zie Voorstel, overweging 11.

[15] Zie bijv. art. 9 (verwerking van bijzondere persoonsgegevens), 17 (uitzondering op het recht om te worden vergeten), 20 (uitzondering op de bepaling inzake profilering), 21 (beperking van de reikwijdte van diverse artikelen van de Verordening), 27 (verplichtingen tot verwerking van gegevens), 44 (afwijkingen van de regels voor doorgifte van persoonsgegevens), 78 (vaststellen van sancties), 81 (verwerking van gezondheidsgegevens), 82 (verwerkingen van gegevens in het kader van de arbeidsverhouding).

[16] 2010/C 83/01. De geconsolideerde versie van het VWEU is beschikbaar via: http://eur-lex.europa.eu/JOHtml.do?uri=OJ:C:2010:083:SOM:NL:HTML.

[17] Art. 16:1 VWEU: "Eenieder heeft recht op bescherming van zijn persoonsgegevens. 2. Het Europees Parlement en de Raad stellen volgens de gewone wetgevingsprocedure de voorschriften vast betreffende de bescherming van natuurlijke personen ten aanzien van de verwerking van persoonsgegevens door de instellingen, organen en instanties van de Unie, alsook door de lidstaten, bij de uitoefening van activiteiten die binnen het toepassingsgebied van het recht van de Unie vallen, alsmede de voorschriften betreffende het vrij

VWEU). Opmerking verdient dat in Nederland de Tweede Kamer de regering heeft verzocht om een parlementair behandelvoorbehoud te laten vastleggen. Dit betekent dat de regering op Europees niveau pas kan instemmen met het Voorstel nadat hierover een specifiek debat met het Nederlandse parlement is gevoerd. Ook de Belgische overheid heeft de nodige stappen ondernomen om het Voorstel te analyseren en het Ministerie van Justitie is alvast gestart met een openbare raadpleging omtrent het Voorstel.[18]
Het Voorstel is op 27 januari 2012 toegezonden aan het Europees Parlement (hierna 'EP') en de Raad. Op het moment van afsluiten van dit artikel wachten wij op de eerste lezing in het EP. Zowel het EP als de Raad kunnen in de eerste lezing tekstwijzigingen voorstellen. Indien de Raad en het EP het niet eens worden over deze amendementen, volgt er een nieuwe behandeling waarbij in tweede lezing opnieuw tekstwijzigingen kunnen worden voorgesteld. Als het EP en de Raad een compromis bereiken, wordt het Voorstel goedgekeurd. Lukt dit niet, dan probeert een bemiddelingscomité nog een oplossing te vinden. Zowel de Raad als het EP kunnen het Voorstel in deze laatste lezing blokkeren. Wanneer het Voorstel wordt aangenomen treedt de Verordening in werking op de twintigste dag na die van de bekendmaking ervan in het *Publicatieblad van de Europese Unie*. De Verordening zal dan van toepassing zijn met ingang van twee jaar na de datum van inwerkingtreding. In Nederland wordt dan de Wet bescherming persoonsgegevens ingetrokken en in België de Privacywet.[19]
Zou daarmee een einde komen aan de periode van gefragmenteerde regelgeving en sanctionering inzake de bescherming van persoonsgegevens?

1. Toepassingsgebied en definities

1.1 Toepassingsgebied

Het materiële toepassingsgebied van het Voorstel komt overeen met het toepassingsgebied van Richtlijn 95/46/EG. Uitgangspunt in het nieuwe art. 2 is nog steeds dat de regels van toepassing zijn op de geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens. Daarnaast zijn de regels van toepassing op niet-geautomatiseerde verwerking van gegevens die in een bestand zijn opgenomen, of bestemd zijn om in een bestand te worden opgenomen. De uitzonderingen op het materiële toepassingsgebied zijn verder gepreciseerd, in het bijzonder de uitzonderingen die betrekking hebben op verwerkingen die vallen buiten het bereik van het gemeenschapsrecht, verwerkingen door EU-instellingen en verwerkingen die vallen binnen de uitvoering van activiteiten op het gebied van het gemeenschappelijke buitenland- en veiligheidsbeleid van de Unie. Uitgezonderd zijn ook nog steeds de verwerkingen door een natuurlijke persoon, uitsluitend voor persoonlijk of huishoudelijk gebruik. Aan deze uitzondering is expliciet toegevoegd dat de uitzondering geldt indien deze verwerkingen plaatsvinden *zonder winstoogmerk*. Van belang is ook de toelichting in overweging 15, dat op deze uitzondering geen beroep kan worden gedaan door verantwoordelijken of verwerkers die aan natuurlijke personen de middelen ter beschikking stellen voor verwerking voor persoonlijk of huishoudelijk gebruik. Daarmee wordt duidelijk dat bijvoorbeeld cloud providers of ook sociale netwerkleveranciers niet kunnen profiteren van deze uitzondering op de werkingssfeer.

---

verkeer van die gegevens. Op de naleving van deze voorschriften wordt toezicht uitgeoefend door onafhankelijke autoriteiten. De op basis van dit artikel vastgestelde voorschriften doen geen afbreuk aan de in artikel 39 van het Verdrag betreffende de Europese Unie bedoelde specifieke voorschriften".

[18] Zie http://justitie.belgium.be/nl/nieuws/andere_berichten/news_2012-03-12.jsp.

[19] Wet van 6 juli 2000, *Stb.* 2000, 302. Gewijzigd bij wet van 5 april 2001, *Stb.* 2001, 180 (Wet bescherming persoonsgegevens) en Wet van 8 december 1992 voor de bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens (Privacywet), zoals gewijzigd bij wet van 11 december 1998.

Het territoriale toepassingsgebied is ingrijpend geherdefinieerd in art. 3 van het Voorstel. Vooropgesteld moet worden dat de bepaling uiteraard aanzienlijk verschilt van art. 4 Richtlijn 95/46/EC, nu niet langer de reikwijdte van het nationaal toepasselijke recht moet worden bepaald. Nu de Verordening naar haar aard rechtstreekse werking heeft in de lidstaten is op het eerste gezicht een aanzienlijke vereenvoudiging bereikt. De bepaling omvat echter diverse nieuwe elementen, die niet zonneklaar zijn, maar naar verwachting leiden tot een verdere uitbreiding van de werkingssfeer. Het Voorstel van Verordening zal conform het art. 3 lid 1 van toepassing zijn op de verwerking van persoonsgegevens in het kader van de activiteiten van een vestiging van een verantwoordelijke of een verwerker in de Unie. De toevoeging 'of een verwerker' is nieuw en vormt de basis voor de nieuwe zelfstandige verplichtingen van verwerkers op grond van het Voorstel. Overweging 19 verduidelijkt dat het Voorstel van Verordening van toepassing zal zijn, ongeacht of de verwerking zelf plaatsvindt in de Unie. Onder de Richtlijn kenden we dit uitgangspunt ook, maar toen betrof deze regel de verantwoordelijke. De toelichting impliceert dat het Voorstel ook gevolgen heeft voor verwerkers die in de Unie zijn gevestigd, maar die de gegevensverwerking uitbesteden aan een andere verwerker (subverwerker) buiten de Unie, zolang de verwerking moet worden aangemerkt als een verwerking 'in het kader van de activiteiten van de vestiging van de verwerker' in de Unie. Aldus zou het Voorstel gevolgen kunnen hebben voor gegevensverwerkingen die anders dan de plaats van de vestiging van de verwerker, geen enkele relatie hebben met de Unie, omdat bijvoorbeeld de opdrachtgevers en de betrokkenen daarbuiten zijn gevestigd, terwijl ook de daadwerkelijke verwerking van de gegevens bij een subverwerker buiten de EU plaatsvindt. Dit punt behoeft verdere verduidelijking.

Ook art. 3 lid 2 omvat nieuwe elementen. Ingevolge lid 2 is het Voorstel van toepassing op de verwerking van persoonsgegevens van betrokkenen woonachtig in de Unie door een verantwoordelijke buiten de Unie, indien de verwerking verband houdt met a. het aanbieden van goederen of diensten aan betrokkenen in de Unie; of b. de monitoring van hun gedrag. Deze bepaling omvat een aanzienlijke uitbreiding van het toepassingsgebied van de EU-regelgeving tot partijen buiten de Unie. Onder het oude art. 4 lid 2 was de extraterritoriale werking 'beperkt' tot verantwoordelijken buiten de Unie die gebruikmaakten van 'middelen' in de Unie. Onder middelen werden mogelijk zowel verwerkers in de Unie verstaan als technische middelen (zoals cookies), zodat de Richtlijn 95/46/EC van toepassing was op websites van aanbieders buiten de Unie die in EU-lidstaten cookies plaatsten. In het nieuwe art. 3 lid 2 wordt de techniek als aanknopingspunt voor het toepasselijke recht verlaten, maar wordt het doel van de verwerking centraal gesteld. Uit overweging 21 volgt dat bij monitoring wordt gedacht aan het volgen van gedrag op het internet en het opstellen van profielen, op basis waarvan beslissingen over een persoon worden genomen, of voorkeuren, gedrag of opvattingen worden bepaald. In zoverre sluit de nieuwe bepaling de facto aan bij de nu geldende situatie. Niet duidelijk is echter of de bepaling inzake 'monitoring' ook betrekking kan hebben op andere activiteiten die als 'monitoring' gekwalificeerd zouden kunnen worden, zoals het opnemen van een telefoongesprek met een klantenservice (call centre) van een aanbieder buiten de Unie of monitoring die met nieuwe technieken zoals 'smart metering' allicht in de toekomst meer ingang zullen vinden. Ook is niet duidelijk of en in hoeverre voor de toepasselijkheid van art. 3 lid 2 onder a het relevant is of de goederen en diensten expliciet aan EU-onderdanen worden aangeboden of dat het voldoende is dat deze diensten (de facto) door EU-onderdanen worden afgenomen. De wetgever zou er goed aan doen om duidelijkheid te verschaffen in de Verordening zelf, eerder dan dit later aan het Hof van Justitie te moeten overlaten. Zo zou de wetgever enkele criteria naar voren kunnen schuiven zoals het gebruik van Europese talen, Europese domeinnaamextensies, Europese munteenheid,

verschepingsmogelijkheden, enz. die kunnen wijzen op een uitdrukkelijk aanbod aan EU-onderdanen.

Daarentegen is het duidelijk dat in de gevallen genoemd in art. 3 lid 2 de verantwoordelijke buiten de Unie op grond van art. 25 in de Unie een vertegenwoordiger moet aanwijzen. Deze vertegenwoordiger handelt namens de verantwoordelijke en kan door iedere toezichthouder worden aangesproken. Op de verplichting om een vertegenwoordiger aan te wijzen gelden volgens het Voorstel enkele uitzonderingen: het aanwijzen van een vertegenwoordiger is niet verplicht als de verantwoordelijke is gevestigd in een land dat naar het oordeel van de Europese Commissie een passend beschermingsniveau waarborgt en ook niet als de verantwoordelijke een klein of middelgroot bedrijf is (dat wil zeggen: minder dan 250 mensen tewerkstelt), of een publieke autoriteit of overheidsorgaan is of als slechts incidenteel goederen of diensten aan betrokkenen in de Unie worden geleverd. Overweging 64 licht toe dat de verantwoordelijke buiten de Unie zich op de laatstgenoemde uitzondering kan beroepen als het evident is dat het aanbieden van goederen of diensten aan betrokkenen in de Unie ondergeschikt is aan de kernactiviteiten van de verantwoordelijke. Voor de goede orde: uit de samenhang van de bepalingen volgt dat de verantwoordelijke in dat geval geen vertegenwoordiger hoeft aan te wijzen, maar overigens wel (zelf) de verplichtingen op grond van de Verordening moet naleven.

1.2 Definities met marginale wijzigingen

In de preambule wordt duidelijk gesteld dat het huidige juridische raamwerk betreffende gegevensbescherming nog steeds solide is voor wat betreft de daarin verankerde doeleinden en beginselen. Door de verschillen in nationale implementatiewetgeving is echter sprake van vergaande fragmentatie met als gevolg rechtsonzekerheid. De herziening richt zich dan ook met name op het bouwen van een sterker en meer coherent Europees juridisch raamwerk waarbij strikte handhaving en controle van betrokkenen over hen betreffende data als belangrijke uitgangspunten gelden. Het is dan ook niet zo verwonderlijk dat met het Voorstel een groot aantal definities uit Richtlijn 95/46/EG zonder wijzigingen zijn overgenomen, of slechts marginaal zijn aangepast of aangevuld met nieuwe elementen.[20] De twee kernconcepten 'betrokkene' en 'persoonsgegevens', welke in art. 2 (a) Richtlijn 95/46/EG waren samengevoegd, zijn in het Voorstel apart gedefinieerd. Hierbij is in de definitie een deel van de uitleg die te vinden was in overweging 26 van de Richtlijn 95/46/EG geïncorporeerd.[21] Hierdoor blijkt nu rechtstreeks uit de definitie dat om te bepalen of een persoon identificeerbaar is, moet worden gekeken naar alle middelen waarvan mag worden aangenomen dat zij redelijkerwijs in te zetten zijn door degene die voor de verwerking verantwoordelijk is dan wel door enig ander persoon om genoemde persoon te identificeren. In Richtlijn 95/46/EG werd hierbij opgemerkt dat identificatie met name kon plaatsvinden aan de hand van een identificatienummer of van een of meer specifieke elementen die kenmerkend zijn voor de fysieke, fysiologische, psychische, economische, culturele of sociale identiteit van de betrokkene. In het Voorstel worden hieraan locatiegegevens en 'online identifiers' alsmede genetische en mentale kenmerken van de betrokkene toegevoegd. Het

[20] Zie art. 4 Voorstel.

[21] In het Voorstel is overweging 26 van Richtlijn 95/46/EG overigens wel behouden (zie overweging 23 Voorstel: "De beschermingsbeginselen moeten voor elk gegeven betreffende een geïdentificeerde of identificeerbare persoon gelden. Om te bepalen of een persoon identificeerbaar is, dienen alle middelen in aanmerking te worden genomen waarvan redelijkerwijs te verwachten valt dat zij door de voor de verwerking verantwoordelijke, of door ieder ander worden gebruikt om de persoon te identificeren. De beschermingsbeginselen dienen niet van toepassing te zijn op gegevens die zodanig anoniem zijn gemaakt dat de persoon op wie die gegevens betrekking hebben, niet meer identificeerbaar is".

begrip ‘persoonsgegevens’ wordt in het Voorstel vervolgens kort gedefinieerd als ‘alle informatie betreffende een betrokkene’. Hierbij volgt uit overweging 23 als aanvullend aspect dat de beginselen van gegevensbescherming niet gelden met betrekking tot gegevens die dusdanig geanonimiseerd zijn waardoor identificatie van de betrokkene niet langer mogelijk is. Wat het begrip identificatienummers, locatiegegevens, online-identificatiemiddelen en andere specifieke factoren betreft, blijkt de wetgever alvast ruimte voor discussie te laten omtrent het al dan niet kwalificeren als persoonsgegeven (overweging 24 bij het Voorstel).
Ook concepten als ‘verwerking van persoonsgegevens’, ‘bestand van persoonsgegevens’, ‘verantwoordelijke’, ‘verwerker’ en ‘ontvanger’ zijn vrijwel ongewijzigd gebleven. Hierbij moet wel worden opgemerkt, zoals later in deze bijdrage ook beschreven wordt, dat het Voorstel wel meer nadrukkelijk ingaat op de rolverdeling tussen verantwoordelijke en verwerker. In het Voorstel is een apart vierde hoofdstuk aan deze rolverdeling gewijd waarbij deels wordt aangehaakt bij art. 17 lid 2 Richtlijn 95/46/EG, waarover hieronder meer. Nieuw is echter de verduidelijking dat een verwerker die niet uitsluitend op instructie van de voor de verwerking verantwoordelijke handelt, als een gezamenlijk voor de verwerking verantwoordelijke beschouwd moet worden in plaats van als verwerker.
De definitie van derde voegde ook in de Richtlijn al weinig toe, dus het schrappen van deze definitie in het Voorstel behoeft geen nadere toelichting.

Het is wel van belang om te wijzen op de nadere precisering van het concept ‘toestemming’. Niet alleen is in de definitie meer richting aan dit concept gegeven, maar het Voorstel gaat in art. 7 nader in op de voorwaarden waaraan een rechtsgeldige toestemming moet voldoen. In de definitie is in het Voorstel toegevoegd dat het moet gaan om een expliciete indicatie van de wensen van de betrokkene. Deze eis geldt naast de ook in Richtlijn 95/46/EG opgesomde vereisten dat het bij toestemming moet gaan om een ‘vrije, specifieke en op informatie berustende wilsuiting’. Bovendien is ten opzichte van de definitie in Richtlijn 95/46/EG in het Voorstel toegevoegd dat de wilsuiting gegeven moet worden ‘door middel van hetzij een verklaring hetzij een ondubbelzinnige actieve handeling’. Vooraf ingevulde ‘voor akkoord’ vakjes zouden hierdoor bijvoorbeeld niet meer rechtsgeldig zijn, zoals overigens ook in overweging 36 van het Voorstel aangegeven. In art. 7 van het Voorstel wordt de bewijslast bovendien uitdrukkelijk bij de verantwoordelijke gelegd, wordt erop gewezen dat indien de toestemming blijkt uit een geschreven document dat ook op andere zaken betrekking heeft dan enkel de toestemming voor gegevensverwerking, de toestemming voor gegevensverwerking duidelijk door de betrokkene onderscheiden moet kunnen worden van de andere zaken die het document betreft. Deze bepaling lijkt geïnspireerd te zijn op eerdere bepalingen in consumentenwetgeving. Het artikel bepaalt bovendien uitdrukkelijk dat de toestemming te allen tijde kan worden ingetrokken, waarbij dit geen gevolgen heeft voor de rechtsgeldigheid van de verwerking van persoonsgegevens vóór het moment dat de toestemming is ingetrokken. Tevens vermeldt art. 7 van het Voorstel dat toestemming geen geldige verwerkingsgrond biedt in die gevallen waarin er duidelijk sprake is van een onevenwichtigheid in de relatie tussen de verantwoordelijke en de betrokkene. Uit verschillende artikelen in het Voorstel blijkt dat hier met name gedacht wordt aan arbeidsrelaties en verwerkingen waarbij kinderen betrokken zijn.

1.3 Nieuwe definities

Naast de hierboven vermelde beperkte wijzigingen in bestaande definities, voegt het Voorstel een flink aantal nieuwe definities toe. Het gaat om: ‘inbreuk in verband met persoonsgegevens’[22], ‘genetische gegevens’, ‘biometrische gegevens’, ‘gegevens over

[22] Het concept ‘inbreuk in verband met persoonsgegevens’ is gebaseerd op art. 2(h) Richtlijn 2002/58/EG (E-privacy Richtlijn) van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van

gezondheid', 'belangrijkste vestiging', 'vertegenwoordiger', 'onderneming', 'groep ondernemingen', 'bindende bedrijfsvoorschriften', 'toezichthoudende autoriteit' en 'kind'. We bespreken hieronder enkele nieuw gedefinieerde categorieën van bijzondere gegevens alsmede de toevoeging van de definitie van kind en specifieke bepalingen met betrekking tot de verwerking van persoonsgegevens van kinderen.

1.3.1 Bijzondere categorieën van gegevens

De soorten gegevens die vallen binnen de definitie van bijzondere persoonsgegevens waarvan de verwerking, weliswaar met heel wat uitzonderingen, verboden is, worden uitgebreid. Hoewel in de Richtlijn 95/46/EG al sprake was van de vermelding van gezondheidsgegevens, worden 'gegevens over gezondheid' in het Voorstel expliciet gedefinieerd als 'alle informatie over de fysieke of mentale gezondheid van een persoon, of over de verlening van een gezondheidsdienst aan een persoon'. Dat deze definitie erg ruim is blijkt uit de opsomming in overweging 26 van het Voorstel. De reden om gezondheidsgegevens nader te specificeren lijkt samen te hangen met een verduidelijking van die situaties waarin gezondheidsgegevens, ondanks het feit dat zij bijzondere gegevens zijn, wel degelijk verwerkt kunnen worden. In overweging 42 wordt gewezen op mogelijkheden voor de verwerking van gezondheidsgegevens in het kader van gezondheidsverzekeringen en ten behoeve van historisch, wetenschappelijk en statistisch onderzoek. De overwegingen 122 en 123 van het Voorstel zien op grensoverschrijdende zorg en op gevallen waarin de verwerking van gezondheidsgegevens zonder toestemming van betrokkenen noodzakelijk is met het oog op het algemeen belang, waarvan de volksgezondheid onderdeel uitmaakt. De inhoud van de overwegingen vindt hun weerslag in art. 81 van het Voorstel.

Naast een explicitering van gezondheidsgegevens, worden de bijzondere categorieën gegevens in het Voorstel uitgebreid met biometrische gegevens en genetische gegevens. Biometrische gegevens worden gedefinieerd als 'alle gegevens met betrekking tot de fysieke, fysiologische of gedragskenmerken van een persoon op grond waarvan de eenduidige kenmerking van die persoon mogelijk is, zoals afbeeldingen van het gezicht of dactyloscopische gegevens'.[23] De Engelstalige tekst daarentegen vermeldt gegevens die toelaten om 'op unieke wijze te identificeren'. Op het eerste zicht is het onduidelijk waarom de definitie enkel de gegevens die 'op unieke wijze identificeren' omvat. Biometrische gegevens worden in toepassingen immers niet steeds gebruikt om te identificeren[24] maar ook om te herkennen door vergelijking.[25] In beide gevallen worden echter biometrische kenmerken ingezameld en opgeslagen, hetgeen een risico inhoudt. Voor bepaalde lichaams- of gedragskenmerken kan ook discussie ontstaan of deze voldoende uniek dan wel eerder

---

persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (Richtlijn 2002/58/EG betreffende privacy en elektronische communicatie) (*PbEG* 31 juli 2002, L 201, p. 37-47) zoals gewijzigd door Richtlijn 2009/136/EG van het Europees Parlement en de Raad van 25 november 2009 tot wijziging van Richtlijn 2002/22/EG inzake de universele dienst en gebruikersrechten met betrekking tot elektronischecommunicatienetwerken en -diensten, Richtlijn 2002/58/EG betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie en Verordening (EG) nr. 2006/2004 betreffende samenwerking tussen de nationale instanties die verantwoordelijk zijn voor handhaving van de wetgeving inzake consumentenbescherming (Voor de EER relevante tekst) (*PbEG* 18 december 2009, L 337, p. 11-36).

[23] Art. 4 (11) Voorstel. Dactyloscopische gegevens verwijzen naar het (forensisch) onderzoek van de vingerafdruklijnen en patronen als methode voor het vaststellen van iemands identiteit.

[24] Identificeren in eigenlijke zin is een antwoord vinden op de vraag wie een persoon is door een gegeven kenmerk te vergelijken met een lijst met kenmerken van verschillende personen, opgeslagen in een databank.

[25] Vergelijken is nagaan of een biometrisch kenmerk (bijv. een vingerafdruk in een paspoort) afkomstig is van dezelfde persoon (bijv. de paspoorthouder) door het (bijv. in het paspoort) opgeslagen biometrisch gegeven te vergelijken met het nieuw gegeven kenmerk (één-op-één vergelijking). In dit geval wordt de persoon niet geïdentificeerd maar herkend.

onderscheidend zijn, zoals bijvoorbeeld de handomtrek. Ten slotte lijkt de definitie zich niet te beperken tot het gebruik van biometrische gegevens, zoals foto's of vingerafdrukken, in automatische toepassingen. De definitie sluit met andere woorden niet het gebruik uit van biometrische gegevens in niet-automatische toepassingen.
De definitie van genetische gegevens in het Voorstel luidt: 'alle gegevens, van welke aard ook, over de overgeërfde of tijdens de vroege prenatale ontwikkeling verkregen kenmerken van een persoon'. Men kan zich de vraag stellen of deze definitie van genetische gegevens niet te ruim is opgevat waardoor alle mogelijke persoonsgegevens die verbonden zijn aan de lichamelijke of geestelijke gesteldheid van een individu als genetische gegevens kwalificeren, zodat bijvoorbeeld ook een eenvoudige foto als genetisch gegeven kwalificeert. Zou dit de bedoeling van de wetgever geweest zijn?

1.3.2 Kinderen

Overweging 29 bij het Voorstel geeft aan waarom kinderen specifieke bescherming verdienen als het om de verwerking van persoonsgegevens gaat, namelijk omdat kinderen zich minder bewust zijn van de risico's, consequenties, waarborgen en rechten met betrekking tot de verwerking van persoonsgegevens. De definitie van kind is gebaseerd op het Verdrag inzake de rechten van het kind waarin het eerste artikel bepaalt: 'Ieder mens jonger dan achttien jaar is een kind'.[26] Ondanks deze definitie, lijkt het Voorstel de extra bescherming voor kinderen echter voor te behouden aan jongere kinderen. Art. 8 van het Voorstel bepaalt in relatie tot 'diensten van de informatiemaatschappij' dat de verwerking van persoonsgegevens betreffende kinderen 'jonger dan 13 jaar' alleen rechtmatig is met de toestemming van de ouders of wettelijk vertegenwoordigers van het kind. Het is aan verantwoordelijken om redelijke inspanningen te verrichten om verifieerbare toetstemming te verkrijgen. In dit verband kan, aldus art. 8 lid 4 de Commissie standaardformulieren opstellen voor specifieke methoden om verifieerbare toestemming te verkrijgen. Een vroegere, gelekte, versie van het Voorstel maakt geen onderscheid tussen kinderen jonger dan 18 jaar en kinderen jonger dan 13 jaar, maar stelde een sterke bescherming in voor alle kinderen jonger dan 18 jaar. In een opinie van de Artikel 29 Werkgroep betreffende gegevensbescherming van kinderen wordt gesteld dat een kind behandeld moet worden naar 'het niveau van volwassenheid van het kind'.[27] Hoewel dit niveau meer kind- dan leeftijdsgebonden is, wordt wel vastgehouden aan het uitgangspunt dat ieder mens jonger dan 18 jaar in beginsel valt onder het specifieke beschermingsregime. Deze uitleg lijkt een betere bescherming te bieden, waarbij de mogelijkheid openblijft om per geval af te wijken. Het is afwachten of de oorspronkelijke versie terug zal opgevist worden in het Europees Parlement of de Raad.
Biometrische gegevens, genetische gegevens en kinderen komen in het Voorstel samen in art. 33. Dit artikel betreft een verplichting om een zogenoemde 'Privacyeffectbeoordeling' ('Privacy Impact Assessment' of 'PIA') te maken. Dit betreft een soort gegevensbeschermingsevaluatie voor verwerkingen van persoonsgegevens waarbij specifieke risico's bestaan voor de rechten en vrijheden van betrokkenen. In lid 2 onder (d) wordt in dit kader expliciet gewezen op: 'de verwerking in grote bestanden van persoonsgegevens inzake kinderen en van genetische of biometrische gegevens'. Later in deze bijdrage komen we terug op de privacyeffectbeoordeling.

1.3.3 Joint controller

[26] Aangenomen door de Algemene Vergadering van de Verenigde Naties op 20 november 1989, beschikbaar via: www.kinderbescherming.nl.
[27] 'Working Document 1/2008 on the protection of children's personal Data, 00483/08/EN, WP 147, adopted on 18 February 2008', beschikbaar via:
http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp147_en.pdf.

Tot slot kan nog gewezen worden op een nieuw concept dat niet met art. 4 van het Voorstel betreffende definities geïntroduceerd wordt, maar in art. 24 van het Voorstel waar het een 'joint controller' ofwel 'gezamenlijk voor de verwerking verantwoordelijken' betreft. Met dit artikel wordt meer duidelijkheid gebracht in de situatie waarin meerdere verantwoordelijken, samen doel en middelen bepalen. In deze situatie moeten de gezamenlijk verantwoordelijken onderling bepalen wie verantwoordelijk is voor de naleving van de rechten en plichten vastgelegd in de Verordening. De nieuw ingevoegde definitie van vertegenwoordiger is te vinden in art. 25 terwijl art. 26 nadere regels geeft over de rolverdeling tussen verantwoordelijke en verwerker. Zoals reeds vermeld, is bepaald dat indien de verwerker verdergaat met de verwerking van persoonsgegevens dan de door de verantwoordelijke gegeven instructies, de verwerker aangemerkt moet worden als gezamenlijk verantwoordelijke in de zin van art. 24. De rolverdeling tussen verantwoordelijken en verwerkers is nader uitgewerkt in hfdst. 4 van het Voorstel. Hierbij is van belang dat uitdrukkelijk is vereist dat een verantwoordelijke beleid voert en passende maatregelen neemt om ervoor zorg te kunnen dragen en aan te kunnen tonen dat in overeenstemming met het recht op gegevensbescherming persoonsgegevens verwerkt worden.[28] Het ten opzichte van de Richtlijn ingevoerde vereiste van ´aan kunnen tonen´ geeft invulling aan het vereiste van accountability. Lid 2 van art. 22 maakt duidelijk dat het beleid en de maatregelen zich met name moeten richten op de documentatieplicht (zie hieronder), beveiligingsplicht, PIA, vereisten om te voldoen aan voorafgaand toezicht of toestemming, en het aanwijzen van een functionaris voor de gegevensverwerking. Op grond van lid 3 van art. 22 moeten de effectiviteit van genomen maatregelen intern of extern getoetst worden, tenzij dit disproportioneel zou zijn. De Commissie is bevoegd nadere criteria en eisen te stellen aan de passende maatregelen en met betrekking tot de mechanismen om de effectiviteit te toetsen. Art. 23 betreft de nieuwe concepten ´privacy by design´ en ´privacy by default´ welke besproken worden in paragraaf 2.2.2. De verwerker wordt meer specifiek beschreven in art. 26, waarvan lid 1 nog een plicht voor de verantwoordelijke betreft, namelijk het kiezen van een verwerker die overeenkomstig de wet zal handelen. De onderlinge verhouding tussen verantwoordelijke en verwerker moet geregeld worden bij contract. Hierbij geldt onder andere dat een verwerker alleen een nieuwe verwerker, eerder ook aangeduid als subverwerker, in mag schakelen met toestemming van de verantwoordelijke.[29] De instructies van de verantwoordelijke aan de verwerker moeten uitdrukkelijk gedocumenteerd worden. Deze instructies zijn van groot belang, aangezien voor handelingen die vallen buiten deze instructies, de verwerker aangemerkt moet worden als verantwoordelijke.[30] Art. 27 maakt duidelijk dat verwerkers, en ieder ander die handelt onder gezag van de verantwoordelijke, alleen persoonsgegevens verwerken in opdracht van de verantwoordelijke, tenzij zij bij wet tot de verwerking zijn verplicht. Op grond van art. 28 hebben verantwoordelijken en verwerkers een documentatieplicht met betrekking tot de verwerking van persoonsgegevens. Deze documentatieplicht draagt bij aan het ´aan kunnen tonen´ van de rechtmatigheid van een verwerking zoals vereist in art. 22. De documentatieplicht is veelomvattend aangezien de documenten betreffende alle verwerkingen die onder hun verantwoordelijkheid hebben plaatsgevonden, bewaard moeten worden. Er wordt tevens een niet-limitatieve lijst gegeven van informatie die de documenten ten minste moeten bevatten. Deze informatie moet op verzoek gedeeld worden met de toezichthoudende autoriteit.[31] Uitgesloten van de documentatieplicht zijn bedrijven met minder dan 250 werknemers waar gegevensverwerking slechts een nevenactiviteit is. Ook met betrekking tot de documentatieplicht geldt dat de

[28] Art. 22 Voorstel.
[29] Art. 26 lid 2 d Voorstel.
[30] Art. 26 lid 3 en 4 Voorstel.
[31] Art. 28 lid 3 Voorstel.

Commissie de bevoegdheid heeft deze nader uit te werken, waarbij de Commissie een standaardformulier vast kan stellen betreffende de documentatieplicht.[32] Tot slot wordt gewezen op art. 29 welke een algemene verplichting voor verantwoordelijken en verwerkers bevat om medewerking te verlenen aan de toezichthoudende autoriteit bij de uitoefening van diens taken. Nu de verplichtingen die gelden met betrekking tot de schriftelijke verantwoording betreffende de rolverdeling tussen verantwoordelijken en verwerkers veel zwaarder is aangezet dan het geval was onder Richtlijn 95/46/EG, zal dit tot gevolg hebben dat veel bestaande overeenkomsten tussen verantwoordelijken en verwerkers aangepast moeten worden en geïnvesteerd zal moeten worden in de handhaving van de documentatieplicht en de toetsing van de effectiviteit van genomen maatregelen.

2. Principes inzake gegevensbescherming

2.1 Herneming van bestaande principes

De bestaande principes voor de verwerking van persoonsgegevens lijken op het eerste gezicht weinig veranderd. Art. 5 van het Voorstel herneemt in grote mate de beginselen van het huidige art. 6 Richtlijn 95/46/EC, weliswaar met enkele subtiele aanpassingen. Zo wordt het beginsel dat persoonsgegevens 'rechtmatig' ('lawfully') en eerlijk ('fairly') moeten verwerkt worden, vervolledigd met de verduidelijking dat de persoonsgegevens voor de betrokkene op een transparante wijze moeten verwerkt worden. Interessant is ook de toevoeging dat het beginsel benadrukt dat slechts een minimum aan gegevens noodzakelijk voor een bepaald doeleinde mogen verwerkt worden (gegevensminimalisatie) en dat persoonsgegevens slechts mogen verwerkt worden als en voor zolang de doeleinden niet kunnen worden vervuld met informatie die niet persoonsgebonden is.[33] Hiermee wordt eigenlijk verwezen naar de verwerking van anonieme gegevens. Het artikel wordt afgesloten met een nieuwe bepaling dat de persoonsgegevens moeten worden verwerkt onder de verantwoordelijkheid en aansprakelijkheid van de verantwoordelijke van de verwerking, die ervoor moet zorgen en zal moeten aantonen dat alle bepalingen voor elke verwerking worden nageleefd.[34] Deze bepaling verwijst naar het beginsel van 'verantwoordelijkheid' van de verantwoordelijke ('accountability') die in het Voorstel wordt benadrukt (zie hieronder).

Interessant zijn ook enkele op het eerste gezicht subtiele wijzigingen vergeleken met het huidige art. 7 Richtlijn 95/46/EC, die evenwel van groot belang zijn. Zo is de titel waaronder het artikel is opgenomen gewijzigd van 'Beginselen betreffende de toelaatbaarheid van gegevensverwerking' naar 'Rechtmatigheid ('lawfulness') van de verwerking'.[35] Hiermee wordt eigenlijk teruggekoppeld naar het reeds bestaande beginsel dat de gegevens 'eerlijk en rechtmatig'[36] moeten worden verwerkt, en dat ook in het Voorstel behouden blijft (zie hierboven). Er worden de laatste tijd echter meer en meer vragen gesteld over de precieze betekenis van 'eerlijk en rechtmatig' en de reikwijdte van de zes gronden, soms ook wel de rechtvaardigingsgronden, grondslagen of wettelijke basis genoemd, van art. 7 Richtlijn 95/46/EC, zoals geïmplementeerd in de nationale wetgevingen. Er bestaat sinds enige tijd meer bepaald discussie[37] over de relatie tussen deze bepalingen, de in art. 7 Richtlijn

[32] Art. 28 lid 5 en 6 Voorstel.
[33] Art. 5 (c) Voorstel.
[34] Art. 5 (f) Voorstel.
[35] Art. 6 Voorstel voorafgegaan door de titel 'Lawfulness of processing'.
[36] Art. 6 1 (a) Richtlijn 95/46/EG.
[37] Zie hieromtrent bijv. ook in Nederland, *Kamerstukken I* 2010/11, 31 051, D inzake Evaluatie Wet bescherming persoonsgegevens ('Motie Franken'). Zie ook het recente zogenaamde *Santander*-arrest van de Hoge Raad in

95/46/EC vermelde gronden en de fundamentele rechten en vrijheden, in het bijzonder art. 8 EVRM.[38] In de rechtspraak, veelal van het Europees Hof voor de Rechten van de Mens in Straatsburg, werden verschillende vereisten uitgewerkt voor inmenging in dit grondrecht, zoals omtrent het vereiste van een wet, noodzaak en de proportionaliteit met het nagestreefde doeleinde. Het Voorstel verwijst nu voor gegevensverwerkingen voor een taak van publiek belang ('public interest') of een taak die deel uitmaakt van de uitoefening van een officiële bevoegdheid ('official authority')[39] uitdrukkelijk naar de vereisten van het bestaan van een wet, een doel van publiek belang ('public interest') of noodzaak ter bescherming van rechten en vrijheden van anderen, en het principe van proportionaliteit met het nagestreefde doeleinde.[40] Deze bepaling is nieuw[41] en wijst op een poging tot een meer allesomvattende benadering van het gegevensbeschermingsrecht.

In de definitie betreffende toestemming is het criterium 'expliciet' toegevoegd om verwarring te voorkomen met de onder Richtlijn 95/46/EG gehanteerde term 'ondubbelzinnige toestemming'. Op deze wijze wordt een enkele consistente definitie van toestemming gehanteerd, waarbij de nadruk ligt op het garanderen dat de betrokkene weet dat, en waarvoor, hij of zij toestemming verleent.[42]

2.2 Nieuwe principes

2.2.1 Naar een nieuwe 'verantwoordelijkheid' voor de verantwoordelijke(n)?

Het Voorstel bevat eveneens een nieuw artikel dat de verantwoordelijkheid[43] van de verantwoordelijke(n) voor de verwerking(en) benadrukt voor het naleven van de Verordening.[44] Zo wordt verduidelijkt dat de verantwoordelijke zal moeten kunnen aantonen dat de wetgeving wordt nageleefd aan de hand van procedures en het implementeren van maatregelen, hetgeen trouwens ook voor de verwerker(s) geldt. Dit omvat onder meer het opstellen en bijhouden van documentatie waarin bijvoorbeeld de verantwoordelijke wordt geïdentificeerd, de doeleinden van de verwerking(en), de (categorieën van) ontvangers van de

---

Nederland (HR 9 september 2011, *LJN* BQ8097), waarbij een verzoek tot verwijdering uit een kredietregistratiebestand centraal stond, en waarin de Hoge Raad stelt dat ondanks de wettelijke basis van een gerechtvaardigd belang van de verantwoordelijke, deze laatste toch altijd een belangenafweging moet maken bij iedere verwerking van persoonsgegevens; over dit arrest, zie M. Jansen, 'Verwerking van persoonsgegevens een inbreuk op artikel 8 EVRM?', *P&I* 2011, p. 299-304; zie ook HvJ 24 november 2011 (*ASNEF et al./Administración del Estado*).

[38] Dit art. 8 EVRM garandeert éénieder het recht op respect voor ondermeer privéleven, familie- en gezinsleven. Par. 2 bepaalt dat geen inmenging van enig openbaar gezag is toegestaan dan bij wet voorzien en indien noodzakelijk in een democratische samenleving voor de daarin genoemde doeleinden, zoals bijv. het voorkomen van wanordelijkheden en strafbare feiten.

[39] In art. 7 (e) Richtlijn 95/46/EG is 'public interest' vertaald als 'algemeen belang' en 'exercise of official authority' door 'uitoefening van het openbaar gezag'.

[40] Art. 6, 3 Voorstel.

[41] Zie hierover ook overweging 36 van het Voorstel, die expliciet vereist dat: "Wanneer de verwerking wordt verricht omdat de voor de verwerking verantwoordelijke hiertoe wettelijk is verplicht of wanneer de verwerking nodig is voor de vervulling van een taak van algemeen belang dan wel voor een taak in het kader van de uitoefening van het openbaar gezag, dient de verwerking een rechtsgrondslag te hebben in de EU-wetgeving of in een wet van de lidstaat die voldoet aan de in het Handvest van de grondrechten van de Europese Unie vervatte vereisten voor beperkingen van de rechten en vrijheden".

[42] Voorstel, p. 8.

[43] In het Engels wordt de discussie soms ook gevoerd onder de noemer van het principe van 'accountability'. Over 'accountability', zie ook Artikel 29 Werkgroep, Opinie 3/2010 (WP 173). Voor een achtergrond van het principe, zie J. Alhadeff, B. Van Alsenoy and J. Dumortier, 'The accountability principle in data protection regulation: origin, development and future directions', paper presented at Privacy and Accountability 2011, international conference, PATS project in Berlin, April 5-6 2011, 27 p., beschikbaar via: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1933731.

[44] Art. 22 Voorstel.

persoonsgegevens, doorgifte naar een 'derde land' en de bewaartermijn van de gegevens worden vermeld. Deze documentatie moet ter beschikking gehouden worden van de toezichthoudende overheden. Deze verplichting is evenwel beperkt tot zogenaamde grote ondernemingen of organisaties van 250 of meer personen. Een kleiner of middelgroot bedrijf ontsnapt evenwel niet indien de gegevensverwerking een hoofdactiviteit is (zie art. 28). Deze documentatieverplichting vervangt eigenlijk in zekere mate de notificatieverplichting van de huidige Richtlijn, die afgeschaft wordt. Verder moeten de verantwoordelijke en de verwerker nu een functionaris voor gegevensbescherming aanstellen (waarover hieronder meer).[45] Het uitvoeren van een privacyeffect- of impactbeoordeling (zie hieronder), voorafgaand overleg en het aanvragen van voorafgaande toelating indien nodig zijn andere maatregelen die expliciet herhaald worden als verplichtingen van de verantwoordelijke. Al deze maatregelen moeten ook effectief zijn, dus uitwerking hebben. Mechanismes moeten ontworpen worden om dit na te gaan, zo nodig via interne of externe audits. De Commissie kan hieromtrent ook nadere regels opleggen.

2.2.2 Gegevensbescherming 'by design' en 'by default'

Nieuw in het Voorstel is de verplichting voor de verantwoordelijke om zowel op het ogenblik van de beslissing omtrent de te gebruiken middelen voor de gegevensverwerking als tijdens de verwerking zelf, gepaste technische en organisatorische middelen en procedures uit te werken om de vereisten van de Verordening en de rechten van de betrokkene te garanderen, rekening houdend met de stand van de techniek en de kostprijs.[46] Dit betekent dat de verantwoordelijke dus reeds in een vroeg stadium, bij het ontwerp, rekening moet houden met de principes en verplichtingen van gegevensbescherming. In het bijzonder wordt gewezen op mechanismes om, 'by default' (dit is bij wijze van uitgangspunt), slechts het minimum van noodzakelijke gegevens voor elk doeleinde in te zamelen en bij te houden. Er dient ook een automatische beperking van de toegang tot de persoonsgegevens ingebouwd te worden.
De Europese Commissie behoudt zich verder het recht voor om in meer specifieke regelgeving overeenkomstig art. 86 verdere criteria te bepalen voor de uitwerking van gegevensbescherming 'by design' voor verschillende sectoren, producten en diensten, evenals technische standaarden.

2.2.3 Kennisgeving van inbreuken

Nieuw in het Voorstel is ook de meldplicht in verband met een inbreuk op persoonsgegevens. Eerder werd een dergelijke meldplicht al geïntroduceerd in de telecommunicatiesector door de Richtlijn 2009/136/EG.[47] In het Voorstel wordt een inbreuk op dezelfde wijze gedefinieerd als in voornoemde Richtlijn, maar uiteraard niet meer beperkt tot de levering van een openbare elektronische communicatiedienst.[48] De nieuwe verplichtingen zien op een inbreuk op de

[45] Art. 35 Voorstel.
[46] Art. 23, 1 Voorstel.
[47] Voor de Richtlijn 2009/136/EG van het Europees Parlement en de Raad van 25 november 2009, zie het concept 'inbreuk in verband met persoonsgegevens' is gebaseerd op art. 2(h) Richtlijn 2002/58/EG (E-privacy Richtlijn) van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (Richtlijn 2002/58/EG betreffende privacy en elektronische communicatie) (*PbEG* 31 juli 2002, L 201, p. 37-47) zoals gewijzigd door Richtlijn 2009/136/EG van het Europees Parlement en de Raad van 25 november 2009 tot wijziging van Richtlijn 2002/22/EG inzake de universele dienst en gebruikersrechten met betrekking tot elektronischecommunicatienetwerken en -diensten, Richtlijn 2002/58/EG betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie en Verordening (EG) nr. 2006/2004 betreffende samenwerking tussen de nationale instanties die verantwoordelijk zijn voor handhaving van de wetgeving inzake consumentenbescherming (Voor de EER relevante tekst) (*PbEG* 18 december 2009, L 337, p. 11-36).
[48] Art. 4 lid 9 Voorstel.

beveiliging die resulteert in een accidentele of onwettige vernietiging, wijziging, niet-geautoriseerde vrijgave van of toegang tot persoonsgegevens die zijn verstuurd, opgeslagen of anderszins verwerkt. Een in populaire termen 'datalek' moet in ieder geval gemeld worden aan de toezichthouder en ook aan de betrokkene indien het lek van persoonsgegevens waarschijnlijk ongunstige gevolgen zal hebben voor de persoonsgegevens of de persoonlijke levenssfeer van de betrokkene.[49] Overweging 67 beschrijft dat een lek waarschijnlijk ongunstige gevolgen zal hebben voor de betrokkene als het lek bijvoorbeeld diefstal van identiteit, fraude, lichamelijk letsel, aanzienlijke vernedering of reputatieschade tot gevolg kan hebben.
De melding aan de betrokkene moet volgens het Voorstel worden gedaan na de melding aan de toezichthouder. De betrokkenen moeten niettemin 'onverwijld' worden geïnformeerd, zodat zij de nodige voorzorgsmaatregelen kunnen treffen.[50] De melding aan de betrokkene kan achterwege blijven als de verantwoordelijke naar tevredenheid van de toezichthouder aantoont dat de gegevens die zijn gelekt door technische maatregelen onbegrijpelijk zijn gemaakt voor iedere persoon die niet bevoegd is kennis te nemen van die gegevens.[51] Overigens dient de verantwoordelijke iedere inbreuk op persoonsgegevens te documenteren. Deze documentatie moet de toezichthouder in staat stellen om de naleving van de verplichtingen in verband met inbreuken op persoonsgegevens in het Voorstel te onderzoeken.[52]
De verplichtingen van de verantwoordelijke worden in het Voorstel nader gedetailleerd en daarmee aangescherpt in vergelijking met de Richtlijn 2009/136/EG. Zo dient een inbreuk op de beveiliging niet alleen 'zonder onnodige vertraging' te worden gemeld aan de toezichthouder, maar waar mogelijk binnen 24 uur nadat de verantwoordelijke de inbreuk heeft opgemerkt.[53] Een melding die later wordt gedaan, moet worden voorzien van een gemotiveerde rechtvaardiging van deze vertraging. Ook wordt de informatie die de verantwoordelijke bij een melding aan de toezichthouder moet verstrekken, gepreciseerd. Zo moet de verantwoordelijke niet alleen de aard van de inbreuk beschrijven, maar ook de categorieën en het aantal van betrokkenen en de categorieën en het aantal datarecords dat aan de inbreuk onderhevig is omschrijven.[54] Op de verwerker rust de verplichting om de verantwoordelijke onmiddellijk op de hoogte te stellen na vaststelling van een inbreuk.[55] De Europese Commissie behoudt zich verder het recht voor om verschillende aspecten nader te regelen, waaronder de criteria en vereisten voor het vaststellen van een inbreuk op persoonsgegevens en de omstandigheden waaronder een verantwoordelijke of een verwerker verplicht is om de inbreuk te melden, en de omstandigheden waaronder een inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor de persoonsgegevens of de persoonlijke levenssfeer van de betrokkene. Daarnaast behoudt de Commissie zich het recht voor om de standaardopmaak voor een melding aan de toezichthouder en de melding aan de betrokkene te bepalen, alsmede de procedures omtrent de meldplicht en de vorm en modaliteit van de hiervoor omschreven documentatie omtrent een inbreuk, inclusief de termijn voor het vernietigen van deze documentatie.[56]

2.2.4 Privacyimpactbeoordeling

[49] Art. 31 en 32 Voorstel.
[50] Dit volgt uit overweging 67 bij het Voorstel.
[51] Art. 32 lid 3 Voorstel.
[52] Art. 31 lid 4 Voorstel.
[53] Art. 31 lid 1 Voorstel.
[54] Art. 31 lid 3 Voorstel.
[55] Art. 31 lid 2 Voorstel.
[56] Art. 31 lid 5 en 6 en art. 32 lid 5 en 6 Voorstel.

Het Voorstel voert een nieuwe verplichting in om een ´privacyeffectbeoordeling´, ook wel ´privacyimpactbeoordeling of 'Privacy Impact Assessment' ('PIA') genoemd, uit te voeren indien de verwerkingen omwille van hun aard, hun omvang of hun doeleinden specifieke risico's inhouden voor de rechten en vrijheden van de betrokkenen.[57]
Het Voorstel somt vijf gevallen op waarin zich dergelijke specifieke risico's voordoen. Het eerste – gebaseerd op het huidige art. 15 lid 1 Richtlijn 95/46/EC – is bij de systematische en uitvoerige evaluatie van persoonlijke aspecten van een natuurlijke persoon of een verwerking voor de analyse of de voorspelling van iemands economische situatie, plaats, gezondheid, persoonlijke voorkeuren, betrouwbaarheid of gedrag, voor zover dit automatisch is en waaraan rechtsgevolgen zijn verbonden of die de persoon in aanmerkelijke mate treft. Een privacyimpactbeoordeling is ook nodig bij de verwerking van gegevens over iemands seksuele leven, gezondheid, ras of etnische oorsprong, of voor de verstrekking van gezondheidsdiensten, epidemiologische onderzoeken, of enquêtes van mentale of besmettelijke ziekten, wanneer de gegevens worden verwerkt om maatregelen of beslissingen te nemen aangaande personen op grote schaal. Het derde en vierde geval gaan respectievelijk over de monitoring van publiek toegankelijke plaatsen, vooral bij gebruik van videocamerabewaking, op grote schaal, en gegevensverwerkingen op grote schaal over kinderen, genetische gegevens of biometrische gegevens. Ten slotte is een privacyeffect- of privacyimpactbeoordeling ook nodig in de gevallen opgesomd door de toezichthoudende autoriteit en die een voorafgaande toelating vereisen. Het Voorstel legt verder op hoe deze PIA moet gebeuren, zij het met de mogelijkheid van verdere verduidelijking in standaarden en procedures die de Commissie kan aannemen.[58] Artikel 34 gebiedt verder dat indien de PIA of de toezichthoudende autoriteit aangeeft dat een verwerking 'waarschijnlijk grote specifieke risico's' met zich meebrengt, de verantwoordelijke of de verwerker de toezichthoudende autoriteit voorafgaandelijk moet raadplegen om toelating te bekomen.

2.2.4 Aanstelling van een functionaris voor gegevensbescherming

De aanstelling van een 'functionaris voor de gegevensbescherming' of 'Data Protection Officer' ('DPO') was onder de Richtlijn niet verplicht, maar een alternatief voor de verplichting om een verwerking van persoonsgegevens te melden aan de toezichthouder. Zoals hiervoor uiteengezet komt de algemene verplichting om een gegevensverwerking te melden aan de toezichthouder te vervallen en daarmee ook de aanstelling van een DPO als 'alternatief' voor de melding. De aanstelling van een DPO wordt nu op grond van art. 35 van het Voorstel verplicht niet alleen voor de verantwoordelijke, maar ook voor een verwerker, waar de verwerking wordt uitgevoerd door: a. een overheidsorgaan of publiekrechtelijke rechtspersoon; b. een bedrijf dat 250 of meer mensen tewerkstelt; c. waar de kernactiviteiten van de verantwoordelijke of de verwerker bestaan uit gegevensverwerkingen die naar hun aard, omvang of hun doeleinden regelmatige en systematische monitoring van betrokkenen vereisen. Bedrijven die voldoen aan de criteria omschreven onder c zullen dus ongeacht hun omvang een DPO moeten aanstellen. Op welke 'kernactiviteiten' de bepaling doelt, is niet zonder meer duidelijk en de overwegingen geven hierop geen toelichting. Mogelijk moet, in lijn met de bijzondere zorg van de Commissie voor het bewaken van de rechten van betrokkenen in de online-omgeving, hier in het bijzonder gedacht worden aan gegevensbrokers of bedrijven die zich richten op het samenstellen van onlineprofielen van internetgebruik. Het is echter niet uitgesloten dat de bepaling een veel verderstrekkende werking heeft.

[57] Art. 33 Voorstel.
[58] Art. 33, 3-33, 7 Voorstel.

De taken van de DPO worden in detail omschreven.[59] In de kern zal de DPO functioneren als een adviseur van de verantwoordelijke of de verwerker en de naleving van de uiteenlopende verplichtingen op grond van het Voorstel bewaken. De verantwoordelijke of verwerker dient de contactgegevens van de DPO te melden aan de toezichthouder en de DPO zal optreden als contactpersoon voor de toezichthouder. Daarnaast zal de PDO ook optreden als contactpersoon voor de betrokkenen, voor alle zaken die betrekking hebben op de verwerking van persoonsgegevens, inclusief de uitoefening van de rechten van de betrokkene. Het is mogelijk dat een groep van ondernemingen of een overheidsinstantie een centrale DPO aanstelt. Bij de aanstelling moet bewaakt worden dat eventuele andere taken van de DPO verenigbaar zijn met de taken en verplichtingen als DPO en geen belangenconflict opleveren. Overigens moet onder meer verzekerd zijn dat de DPO professioneel gekwalificeerd is om het werk uit te voeren, onafhankelijk kan opereren en voldoende middelen ter beschikking heeft om het werk uit te voeren. Het is mogelijk om een DPO in dienst te nemen, maar ook mogelijk om de diensten van een externe DPO in te huren. Een DPO moet worden aangesteld voor ten minste twee jaar en kan worden herbenoemd. Een DPO die in dienst is mag alleen worden ontslagen indien deze niet langer voldoet aan de voorwaarden voor de uitvoering van zijn of haar taken.

2.2.5 Gedragscodes en certificeringsmechanismes

Het Voorstel herneemt eveneens in zekere mate de bepalingen uit de Richtlijn 95/46/EG omtrent gedragscodes en voegt daaraan de bevordering van de vaststelling van certificeringsmechanismes toe.[60] Tijdens de voorbije zeventien jaar is slechts in beperkte mate gebruikgemaakt van de mogelijkheid die gedragscodes bieden.[61] De Commissie blijft echter van oordeel dat gedragscodes de toepassing van de Verordening kunnen bevorderen, in het bijzonder de bepalingen omtrent eerlijke en transparante gegevensverwerking, de inzameling van de gegevens, de informatie aan het publiek en betrokkenen, inclusief aan kinderen, de uitoefening van rechten en de doorgifte van gegevens. De codes dienen ook in mechanismes te voorzien voor toezicht op de naleving van de code en procedures voor geschillenbeslechting. Zoals ook al eerder in de Richtlijn 95/46/EG voorzien, kunnen ontwerp van codes voor advies voorgelegd worden aan de toezichthoudende autoriteiten. Ze kunnen ook algemeen geldig worden verklaard binnen de Unie volgens procedures voorzien door de Commissie.

Wel nieuw is dat het Voorstel nu ook bepaalt dat lidstaten en de Commissie certificeringsmechanismes dienen te bevorderen, inclusief gegevensbeschermingszegels en -merktekens ('Privacy seals'). Allicht dienden een aantal initiatieven en projecten van toezichthoudende autoriteiten als inspiratie voor de opname van deze bepaling.[62] De Commissie behoudt hier eveneens het recht voor om nadere criteria, vereisten en technische normen vast te leggen.[63]

2.3 Nieuwe rechten van betrokkenen

2.3.1 Recht op vergetelheid

De ontwerpverordening introduceert een recht op vergetelheid.[64] Dit recht om vergeten te worden spreekt tot de verbeelding en heeft de laatste maanden dan ook voor geanimeerde

[59] Art. 37 Voorstel.
[60] Art. 38 Voorstel.
[61] Op Europees niveau hebben organisaties zoals IATA, die een sector vertegenwoordigen, gebruikgemaakt van de mogelijkheid om een gedragscode te laten valideren door de Artikel 29 Werkgroep.
[62] Dergelijke initiatief is bijv. EuroPrise. Hierover is (in het Engels) meer te vinden op www.european-privacy-seal.eu/about-europrise.
[63] Art. 39 Voorstel.
[64] Art. 17 Voorstel.

Field Code Changed

publieke debatten gezorgd in de media. Het Voorstel geeft de betrokkene het recht te eisen dat de verantwoordelijke niet alleen zijn persoonsgegevens wist maar tevens zorgt dat deze niet meer verder verspreid kunnen worden. Dit recht is echter enkel onder bepaalde voorwaarden van toepassing, bijvoorbeeld wanneer de gegevens niet meer noodzakelijk zijn voor de verwerking of wanneer de betrokkene zijn toestemming heeft ingetrokken.
De bedoeling van de wetgever is om in het bijzonder ('especially') kinderen te beschermen die wellicht niet zo zorgvuldig omspringen met het beschikbaar maken van hun persoonsgegevens. De Nederlandse vertaling van de passage lijkt, wellicht onbedoeld, het recht op vergetelheid te limiteren tot kinderen door het woord 'met name' te hanteren.
Opmerkenswaardig is dat wanneer de verantwoordelijke de persoonsgegevens openbaar heeft gemaakt, deze tevens alle redelijke maatregelen, waaronder technische maatregelen, moet nemen om ervoor te zorgen dat derde partijen die de gegevens eveneens verwerken op de hoogte gebracht worden van de aanspraak op vergetelheid van de betrokkene. Deze derde partijen zal verzocht worden om iedere koppeling naar, of kopie of reproductie van die persoonsgegevens te wissen.
De eerder gelekte tekst was op dit vlak trouwens veel strenger opgesteld en verplichtte de verantwoordelijke om zelf alle nodige stappen te ondernemen dat enige publieke internetlink, kopie of andere publieke replicatie onmogelijk zou worden gemaakt. Het wordt uitkijken naar de bespreking in de Raad en het Parlement of en in welke mate de bepalingen van de gelekte versie terug ingang gaan vinden.
Interessant is dat in de publieke debatten de Europese wetgever zich vooral richtte op de activiteiten van de sociale netwerken om de introductie van dit recht op vergetelheid te rechtvaardigen. Sinds de publicatie van het Voorstel hebben sociale netwerken echter al meegedeeld dat zij zich niet aangesproken voelen door deze bepaling. Zij menen namelijk niet zelf als verantwoordelijke op te treden voor het merendeel van de persoonsgegevens die op het platform gepubliceerd zijn. Het zouden met name de eindgebruikers zelf zijn die in hun hoedanigheid van verantwoordelijke gegevens plaatsen en verder bewerken. Verwacht mag worden dat de wetgever hier verduidelijking zal scheppen in de finale tekst.
De wetgever heeft getracht om de juiste balans te vinden tussen het recht van de betrokkene om vergeten te worden en het recht van de maatschappij op vrijheid van informatie en meningsuiting. Daarom werden er enkele regels ingevoegd die de verantwoordelijke de mogelijkheid moet geven om alsnog geen gevolg te geven aan de eis van de betrokkene, of om de gegevensverwerking te beperken in plaats van volledig te wissen. Men mag verwachten dat deze oefening tot kopzorgen zal leiden. Een verkeerde of onnauwkeurige inschatting zou immers kunnen leiden tot zware geldboetes oplopend tot 1% van de jaarlijkse wereldwijde omzet van de onderneming.[65]

2.3.2 Recht op gegevensoverdraagbaarheid

Naar analogie met het reeds bestaande recht op nummeroverdraagbaarheid bij telefoniediensten, wordt er nu een algemeen recht op gegevensoverdraagbaarheid geïntroduceerd.[66] Het nieuwe recht laat toe dat de betrokkene van de verantwoordelijke mag eisen dat hem een kopie ter beschikking wordt gesteld van zijn persoonsgegevens, voor zover deze gegevens elektronisch en in een gestructureerd en algemeen gebruikt formaat verwerkt worden. Deze kopie dient te worden aangeleverd in een elektronisch en gestructureerd formaat dat algemeen wordt gebruikt en verder door de betrokkene kan worden gebruikt. De bedoeling van deze bepaling is om betrokkenen die actief zijn op sociale netwerken en andere platforms (plaatsen van foto's, video's, mailberichten en andere data) toe te laten op een eenvoudige wijze van dienstverlener te veranderen. Men kan zich echter de vraag stellen of de

[65] Art. 79, 5 Voorstel.
[66] Art. 18 Voorstel.

wetgever nog aan zijn bedoeling tegemoetkomt met de huidige formulering van het artikel. Door het toepassingsgebied te beperken tot gegevens die in een gestructureerd en algemeen formaat verwerkt worden, valt te betwijfelen of de vele *User Generated Content* die door eindgebruikers op platformen wordt geplaatst nog valt onder de genoemde bepaling. De gelekte tekst bevatte de genoemde beperking niet. Het zou ons dan ook niet verwonderen mocht het Europees Parlement nog proberen de bepaling terug te verbreden.
Het recht van gegevensoverdraagbaarheid is niet beperkt tot het verkrijgen van een kopie van de persoonsgegevens, maar laat tevens toe dat de betrokkene kan eisen dat de persoonsgegevens en ´alle andere informatie die hij heeft verstrekt´ naar een andere dienstverlener worden overgedragen. De gegevens zullen in dit geval in een algemeen gebruikt elektronisch formaat moeten worden overgedragen zodat ongestructureerde ´rommel´ niet zal volstaan. Vreemd is dat het recht beperkt is tot gegevens die de betrokkene zelf heeft verstrekt en voor zover de verwerking op basis van toestemming of een overeenkomst plaatsvindt. Het lijkt onduidelijk te zijn waarom de wetgever een onderscheid heeft willen aanbrengen in toepassingsvoorwaarden wat enerzijds het verkrijgen van een kopie betreft en anderzijds het doen overdragen aan een derde dienstverlener van de gegevens.

3. Doorgifte van persoonsgegevens

De regels voor doorgifte van persoonsgegevens onder Richtlijn 95/46/EG worden vervangen door een meer gedetailleerde, tamelijk complexe regeling. Het uitgangspunt van de regeling is vastgelegd in art. 40: doorgifte van persoonsgegevens naar een ‘derde land’ of een internationale organisatie is alleen toegestaan als de voorschriften voor doorgifte worden nageleefd door de verantwoordelijke en de verwerker, inclusief de eventuele verdere verstrekking (‘onward transfer’) van persoonsgegevens van een derde land of een internationale organisatie naar weer een derde land of internationale organisatie. In de afgelopen jaren is duidelijk geworden dat de praktijk van de doorgifte van persoonsgegevens zich niet eenvoudig liet vangen in de basisregels die de Commissie had geformuleerd in art. 25 en 26 Richtlijn 95/46/EG. De doorgifte van persoonsgegevens naar internationale instanties, de doorgifte door verwerkers en de ‘onward transfer’ waren daarvan slechts enkele voorbeelden, die de Commissie nu kennelijk beoogt te vatten door ze expliciet te benoemen in de algemene bepaling.
Doorgifte mag plaatsvinden indien, kort samengevat, de Europese Commissie heeft besloten dat een ‘passend beschermingsniveau’ bestaat (art. 41) of adequate waarborgen worden geboden voor de doorgifte (art. 42) of de doorgifte wordt gebaseerd op ‘bindende bedrijfsvoorschriften’ doorgaans aangeduid als ‘binding corporate rules’ (art. 43), of een beroep kan worden gedaan op een uitzonderingsbepaling (art. 44).
Zogenoemde ‘adequacy decisions’ (besluiten dat sprake is van een passend beschermingsniveau) van de Europese Commissie kunnen niet langer uitsluitend ten aanzien van een land worden genomen, maar ook ten aanzien van een specifiek grondgebied of een sector voor gegevensverwerking binnen dat land en ook ten aanzien van een bepaalde internationale organisatie. Onomwonden stelt art. 41 dat in geval van een ‘adequacy decision’ voor de doorgifte verder geen voorafgaande autorisatie dient te worden vereist. Art. 41 omschrijft verder in meer detail op welke wijze een ‘adequacy decision’ tot stand komt. Opmerking verdient dat de Europese Commissie ook tot het besluit kan komen dat *geen* sprake is van een passend beschermingsniveau. In dat geval wordt de doorgifte van persoonsgegevens naar een land, grondgebied of sector in dat land of internationale organisatie verboden. Een negatief oordeel van de Europese Commissie over het

beschermingsniveau in een bepaald land is overigens ook mogelijk onder Richtlijn 95/46/EG, maar is in de 17 jaar die zijn verstreken nooit aan de orde geweest. De oordelen van de Commissie, zowel de positieve als de negatieve oordelen, zullen worden gepubliceerd in het *Publicatieblad van de Europese Unie*.
Doorgifte mag ook plaatsvinden als er adequate waarborgen zijn getroffen voor de bescherming van persoonsgegevens, in de vorm van een juridisch-bindend instrument. Het Voorstel noemt voorbeelden van juridisch-bindende instrumenten: a. binding corporate rules (nader uitgewerkt in art. 43); b. door de Europese Commissie goedgekeurde modelcontractbepalingen voor doorgifte van persoonsgegevens; c. modelcontractbepalingen die zijn aanvaard door een toezichthouder conform het consistentiemechanisme indien deze door de Commissie algemeen geldig zijn verklaard; d. contractbepalingen tussen de verantwoordelijke of verwerker en de ontvanger van gegevens die zijn goedgekeurd door een toezichthouder al dan niet na toepassing van het consistentiemechanisme.[67] Het Voorstel noemt nog een mogelijkheid: indien de doorgifte niet wordt gebaseerd op een juridisch-bindend instrument, kan de verantwoordelijke of verwerker voorafgaande autorisatie vragen aan de toezichthouder.[68] De autorisatie kan door de toezichthouder worden verleend, al dan niet na toepassing van het consistentiemechanisme.
De uitzonderingen op de regels voor doorgifte zijn eveneens relevant voor de praktijk.[69] Deze uitzonderingen sluiten voor het grootste deel aan bij de tekst van art. 26 Richtlijn 95/46/EG. Nieuw is dat doorgifte toegestaan kan zijn indien de doorgifte noodzakelijk is voor het gerechtvaardigd belang van de verantwoordelijke of de verwerker. Aan toepassing van deze laatste uitzondering, waarop overigens geen beroep kan worden gedaan door overheidsinstanties, zijn diverse voorwaarden verbonden: beroep op de uitzondering is alleen mogelijk als de doorgifte niet frequent plaatsvindt en niet omvangrijk is en op voorwaarde dat de verantwoordelijke of de verwerker op basis van een risico- assessment waar noodzakelijk passende garanties biedt voor de bescherming van de persoonsgegevens. Het risico-assessment moet worden gedocumenteerd en de toezichthouder moet op de hoogte worden gesteld van deze doorgifte. De Europese Commissie behoudt zich verder het recht voor om de 'gewichtige redenen van algemeen belang' en de 'passende garanties' nader te regelen.[70]
Het Voorstel biedt geen oplossing voor de in de praktijk als problematisch ervaren vorderingen tot verstrekking van gegevens aan buitenlandse toezichthouders en autoriteiten, bijvoorbeeld op grond van de USA Patriot Act[71] in de Verenigde Staten. Verantwoordelijken en verwerkers raken hier gekneld tussen de verplichtingen inzake doorgifte van persoonsgegevens enerzijds en dwingende verplichtingen tot verstrekking aan buitenlandse autoriteiten en toezichthouders anderzijds. Dit is ook opgemerkt door het Nederlands College bescherming persoonsgegevens, dat voorstelt om de bepaling op te nemen die in een eerder uitgelekte versie van het Voorstel was opgenomen, en op grond waarvan de verstrekking via een internationaal rechtshulpverdrag of een internationale overeenkomst diende te worden geregeld.[72] Overigens biedt ook een dergelijke bepaling voor de prakijk allicht nog onvoldoende soulaas.

[67] Art. 42 lid 2 Voorstel.
[68] Art. 42 lid 5 Voorstel.
[69] Art. 44 Voorstel.
[70] Art. 44, 7 Voorstel.
[71] USA Patriot Act is een acroniem voor Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism.
[72] Brief van het CBP d.d. 2 maart 2012 aan de Leden van de Vaste Commissie voor Veiligheid en Justitie en de leden van de Vaste Commissie voor Binnenlandse Zaken van de Tweede Kamer der Staten-Generaal. Zs2011-01054/z2012-00164, p. 4.

4. Versterking van de Toezichthoudende Autoriteiten

De verplichting voor de lidstaten om een overheidsinstantie verantwoordelijk te maken voor het toezicht op de naleving van de Verordening is vastgelegd in art. 46, waarin tevens een plicht is opgenomen voor toezichthoudende autoriteiten om samen te werken. Alvorens in te gaan op de versterking van de toezichthoudende autoriteiten op nationaal niveau, wordt eerst kort ingegaan op een belangrijke wijzigingen op Europees niveau, het vervangen van de Groep Gegevensbescherming Artikel 29 door het Europees Comité voor gegevensbescherming. De art. 64-71 bieden een gedetailleerde beschrijving van de samenstelling, onafhankelijkheid en taken van het Comité. Binnen het takenpakket vallen adviseren over onder andere voorgestelde wetswijzigingen en ontwerpbesluiten, onderzoeken of de rechten en plichten uit de Verordening worden nageleefd, evalueren van praktische toepassing, bevorderen van samenwerking, opleiding en kennisuitwisseling. Ook zijn een bepaling over de beslissingsprocedure, een rapportageplicht en vertrouwelijkheid opgenomen. Uit de beschrijving van de voorzitter (art. 69) en het secretariaat (art. 70) blijkt een zeer nauwe verwevenheid tussen het Europees Comité voor gegevensbescherming en de Europese Toezichthouder voor gegevensbescherming.[73] Deze bundeling van krachten kan een positieve uitwerking hebben op eenduidige uitleg en handhaving van de Verordening.
Het versterken van handhaving wordt mede voorzien door het beter waarborgen van de onafhankelijkheid van de nationale toezichthoudende autoriteiten (art. 47 e.v.) en het uitbreiden van de bevoegdheden van deze autoriteiten (art. 51 e.v.). Het versterken van het vereiste van onafhankelijkheid strookt met de uitspraak van het Hof in de zaak *Commissie/Duitsland* waar een hoge standaard voor onafhankelijkheid is geformuleerd.[74] In dit verband bepaalt art. 46 lid 2 dat wanneer één lidstaat meerdere toezichthoudende autoriteiten heeft, er één wordt aangewezen als enig contactpunt voor de effectieve deelname van die autoriteiten aan het Europees Comité voor gegevensverwerking. De toezichthoudende autoriteit is bevoegd op het grondgebied waar zij is gevestigd. Om te voorkomen dat een verantwoordelijke die opereert in verschillende lidstaten valt onder het toezicht van verschillende autoriteiten is bepaald dat indien een verantwoordelijke of een verwerker vestigingen in verschillende lidstaten heeft, de toezichthoudende autoriteit van de belangrijkste vestiging bevoegd is voor het toezicht op de verwerkingen van de verantwoordelijke en de verwerker in alle lidstaten.[75] Dit met uitzondering van het toezicht op de verwerking van persoonsgegevens door gerechtelijke instanties in het kader van hun gerechtelijke taken (art. 51 lid 3). Ter bevordering van de samenwerking tussen verschillende toezichthoudende autoriteiten leggen art. 55 en 56 verplichtingen op in het kader van wederzijdse bijstand en gezamenlijke handhaving. De taken die op elke toezichthoudende autoriteit afzonderlijk rusten zijn gespecificeerd in art. 52, dat blijk geeft van een zeer breed takenpakket. Toezichthoudende autoriteiten zullen hier enkel deugdelijke uitvoering aan kunnen geven indien hiervoor voldoende budget beschikbaar is. Met betrekking tot budget volstaat de Verordening echter met een zeer open geformuleerde verplichting dat lidstaten er zorg voor moeten dragen dat de toezichthoudende autoriteit kan beschikken over passende menselijke, technische en financiële middelen, alsmede over de benodigde huisvesting en infrastructuur om haar taken en bevoegdheden effectief uit te kunnen voeren en uit te kunnen

[73] Zie voor deze toezichthouder: www.edps.europa.eu/EDPSWEB/.
[74] HvJ EU 9 maart 2010, nr. C-518/07.
http://curia.europa.eu/jurisp/cgi-bin/form.pl?lang=nl&Submit=Zoeken&numaff=C-518/07. Zie voor een noot van Overkleeft-Verburg www.overkleeft-verburg.nl/PDFs/EU%20HvJ%209%20maart%202010%20Toezicht%20inzake%20bescherming%20van%20persoonsgegevens.pdf.
[75] Art. 51 lid 2 Voorstel.

oefenen (art. 47 lid 5). De bevoegdheden van de toezichthoudende autoriteiten zijn beschreven in art. 53, waarvan lid 1 luidt: "*Elke toezichthoudende autoriteit is bevoegd om: (…)*". Doordat woorden als ´ten minste´ of ´met name´ missen is duidelijk dat de opsomming die volgt van limitatieve aard is en dus een hoge mate van harmonisatie is beoogd.

5. Handhaving en sancties

Zoals hierboven aangegeven bieden art. 55 en 56 een verstevigde basis voor samenwerking tussen toezichthoudende autoriteiten. In dit kader geldt de zogenaamde conformiteitstoets welke in art. 57 beschreven is als: "*Voor de in artikel 46, lid 1, genoemde doeleinden werken de toezichthoudende autoriteiten in het kader van de in deze afdeling beschreven conformiteitstoets samen met elkaar en met de Commissie*." Een goede samenwerking is noodzakelijk om ook over de landsgrenzen heen een effectieve handhaving van het gegevensbeschermingsrecht te garanderen. In het Voorstel is een termijn opgenomen van een maand waarbinnen toezichthoudende autoriteiten moeten voldoen aan verzoeken tot wederzijdse bijstand of handhaving van een andere toezichthoudende autoriteit. Indien niet binnen deze termijn gereageerd wordt, is de verzoekende autoriteit bevoegd op het grondgebied van de te laat reagerende toezichthoudende autoriteit om een voorlopige maatregel te nemen. Voor sommige maatregelen die een toezichthoudende autoriteit kan nemen, geldt dat eerst een ontwerpmaatregel voorgelegd moet worden aan het Europees Comité voor gegevensbescherming en de Commissie.[76] De Commissie kan naar aanleiding van het voorleggen van een ontwerpmaatregel advies uitbrengen (art. 59), maar kan ook, met redenen omkleed, een ontwerpmaatregel schorsen. Een toezichthoudende autoriteit kan in geval van buitengewone omstandigheden ook een spoedprocedure starten op basis waarvan voor een bepaalde periode een voorlopige maatregel genomen kan worden. Tevens kan om een dringend advies verzocht worden, hetgeen inhoudt dat het Europees Comité voor gegevensbescherming binnen twee weken met gewone meerderheid van stemmen een advies moet uitbrengen.[77] De Commissie is op basis van art. 62 bevoegd om uitvoeringshandelingen vast te stellen. Uitvoerbare maatregelen van toezichthoudende autoriteiten worden ten uitvoer gelegd in alle lidstaten, tenzij met betrekking tot de ontwerpmaatregel de conformiteitstoetsing niet is nageleefd. Het Voorstel roept niet alleen vragen op vanuit het perspectief van soevereiniteit van de lidstaten, maar plaatst ook vraagtekens bij de onafhankelijkheid van de toezichthoudende autoriteiten ten opzichte van de Commissie.
Het sluitstuk van handhaving, de mogelijkheid van het verkrijgen van schadevergoeding en het opleggen van sancties, is geregeld in art. 73 e.v. De kritiek die in het kader van Richtlijn 95/46/EG geuit werd met betrekking tot het gebrek aan harmonisatie op het terrein van handhaving, is met de Verordening ter harte genomen. Op grond van art. 73 kunnen betrokkenen een klacht indienen bij willekeurig welke toezichthoudende autoriteit. Dit recht geldt ook voor organisaties die de belangen van betrokkenen behartigen. Art. 73 biedt de mogelijkheid om beroep in te stellen tegen besluiten van toezichthoudende autoriteiten en om beroep in te stellen teneinde een toezichthoudende autoriteit te bewegen gevolg te geven aan een klacht. Naast klagen bij toezichthoudende autoriteiten staat de gerechtelijke weg open (art. 74). Hierbij is het nog van belang om erop te wijzen dat individuen verantwoordelijken en verwerkers voor het gerecht kunnen brengen van de lidstaat waar zij gevestigd zijn, dus niet alleen de lidstaat waar de belangrijkste vestiging is, en voor het gerecht van de lidstaat

[76] Art. 58 Voorstel.
[77] Art. 61 Voorstel.

waar de klager woonachtig is. Dit met uitzondering van zaken tegen verantwoordelijken die optreden in de uitoefening van het overheidsgezag (art. 75 lid 2).
Het recht op schadevergoeding is vastgelegd in art. 77. In beginsel zijn zowel de verantwoordelijke als de verwerker(s) hoofdelijk aan te spreken voor het gehele bedrag aan schadevergoeding. Een partij kan zich enkel kwijten van de plicht tot schadevergoeding als hij kan bewijzen dat de schade hem niet kan worden toegerekend. Naast deze hoofdelijke aansprakelijkheid draagt ook de hoogte van het schadebedrag bij aan meer effectieve rechtsbescherming. Hoewel in art. 78 het aan de lidstaten gelaten wordt om regels te stellen inzake sancties, worden in art. 79 betreffende administratieve sancties duidelijke richtlijnen gegeven waarbij boetebedragen worden genoemd van € 250.000 of 0,5%, € 500.000 of 1% of € 1.000.000 of 2% van de jaarlijkse wereldwijde omzet van de verantwoordelijke en/of verwerker die in overtreding zijn van de bij de Verordening gestelde regels. Art. 79 bevat met name een lange lijst van overtredingen waarop het hoogste boetebedrag van toepassing is.
Relevant om te melden is nog dat ook de vertegenwoordiger niet gevrijwaard is van aansprakelijkheidsrisico´s. Art. 78 lid 2 bepaalt dat alle sancties op de vertegenwoordiger worden toegepast, onverminderd de sanctieprocedures die tegen de verantwoordelijke kunnen worden ingesteld.

6. Voorlopige conclusies en kritiek op het Voorstel

De Europese Commissie heeft met het Voorstel duidelijk getracht om aan een aantal bekommernissen tegemoet te komen. Zij is echter met het nu voorliggende Voorstel niet volledig geslaagd in haar opzet. Het Voorstel is zeker nog niet matuur en dient duidelijk nog verder bijgeschaafd te worden om haar doel te bereiken: een geharmoniseerd, gebalanceerd, eenduidig en eenvoudig rechtskader bieden voor het verwerken van persoonsgegevens in een geglobaliseerde informatiemaatschappij.
Op verschillende vlakken kan bovendien kritiek geuit worden op het Voorstel. Wij beperken ons hier tot drie uiteenlopende punten die van grote invloed zullen zijn op de praktische uitwerking van het Voorstel van Verordening. Ten eerste kan gewezen worden op de lengte en complexiteit van het Voorstel welke niet bijdragen aan een eenvoudige praktische toepassing van het juridische kader. Met 91 artikelen is het Voorstel al zeer veelomvattend, en hiermee is niet alles gezegd. De Commissie behoudt zich immers het recht voor om verschillende aspecten nader te regelen in meer specifiek aan te nemen regelgeving, zoals wanneer de verantwoordelijke zijn verwerking baseert op een noodzaak van verwerking voor eigen legitieme belangen[78], omtrent de verantwoordelijkheid van de verantwoordelijke, de criteria en vereisten voor gegevensbescherming ‘by design’ en ‘by default’[79], de criteria en vereisten voor het vaststellen van een inbreuk op persoonsgegevens, inclusief de standaardopmaak voor een melding van een inbreuk, standaarden en procedures voor de PIA[80], en omtrent nadere invulling van de criteria en de vereisten voor de methoden ter verkrijging van verifieerbare toestemming, waarvoor de Commissie eveneens standaardformulieren kan vaststellen.[81]
Ten tweede hebben we een punt van kritiek betreffende de inhoud. Het is bemoedigend dat vele bestaande principes die hun nut bewezen hebben, zoals omtrent de noodzaak van wettige gronden, doelbinding en informatie, behouden blijven, en hier en daar zelfs verduidelijkt of versterkt worden. Toch is het in dit stadium onzeker of het Voorstel in haar ambitie om een

[78] Art. 6,1 (f) and 6, 5 Voorstel.
[79] Art. 23, 3 Voorstel.
[80] Art. 33, 7 Voorstel.
[81] Art. 8 lid 3 en 4 Voorstel.

antwoord te bieden op de uitdagingen die recente nieuwe technologieën stellen, zal slagen. Zo kan men zich afvragen of het Voorstel een voldoende kader biedt voor technologieën zoals RFID, biometrie, locatiegegevens of 'cloud computing'. Vooralsnog lijkt het Voorstel weinig houvast te bieden voor specifieke toepassingen en het is afwachten of de Commissie hier verbetering in brengt middels haar bevoegdheid om nadere regels op te leggen.
Ten derde een punt van kritiek betreffende harmonisatie. Alhoewel implementatie van de Verordening in nationale wetgeving van de lidstaten niet meer nodig zal zijn, kan men zich afvragen of de Verordening nationale interpretaties van gegevensbeschermingsbeginselen, -begrippen en -verplichtingen, zoals die tot op heden vaak een geharmoniseerde aanpak in de weg stonden, zal uitsluiten. De toepassing van de Verordening zal nog steeds vaak gebeuren in een nationale context, waar tradities in interpretaties belangrijk zijn. Deze zullen allicht slechts na meer rechtspraak van het Hof van Justitie en het Europees Hof voor de Rechten van de Mens uitgevlakt worden. Echter ook voor deze hoven geldt dat zij in zekere mate rekening moeten houden met nationale opvattingen. Bovendien laat het Voorstel op veel plaatsen mogelijkheden open voor nationale lidstaten om toch nationale wetgeving uit te vaardigen hetgeen indruist tegen de hele idee van totale harmonisatie dat steekt achter het Voorstel voor een Verordening.